

Claims

[c1] What is claimed is:

1. A network address translation (NAT)–enabled device comprising:

a NAT facility for connecting at least two hosts inside a first network to a second network, wherein the NAT facility allows the inside hosts to share an address of the second network;

a gateway interface for connecting to a demilitarized zone (DMZ) host inside the first network;

a disposer connected to the gateway interface for assigning an address of the second network to the DMZ host; and

a dispatcher connected to the gateway interface and the NAT facility for communicating messages between the second network and the gateway interface or the NAT facility according to a communication criteria of the message.

[c2] 2. The NAT–enabled device of claim1 wherein the communication criteria is derived from a medium access control (MAC) address of the message.

[c3] 3. The NAT–enabled device of claim 2 wherein the dis–

poser assigns the second network address of the NAT-enabled device to the DMZ host if such address is public.

[c4] 4. The NAT-enabled device of claim 3 wherein the disposer assigns a temporary second network address and associated validity lifetime to the DMZ host if the second address of the NAT-enabled device is not public.

[c5] 5. The NAT-enabled device of claim 4 wherein the disposer assigns an address to the DMZ host in response to a request from the DMZ host.

[c6] 6. The NAT-enabled device of claim 5 wherein the disposer allows the DMZ host to acquire a validity lifetime to transmit messages or obtain addresses of hosts in the second network upon a request by the DMZ host.

[c7] 7. The NAT-enabled device of claim 2 wherein the dispatcher stores the address of the DMZ host and compares destination address information of a message received from the second network with the address of the DMZ host, forwarding the message to the DMZ host when the MAC address corresponds to the DMZ host and forwarding the message to the NAT facility when the MAC address does not correspond to the DMZ host.

[c8] 8. The NAT-enabled device of claim 7 wherein the dispatcher identifies a message being sent to the second

network from the DMZ host by checking the MAC address of such message.

- [c9] 9. A network address translation (NAT)-enabled device comprising:
- a NAT facility for connecting at least two hosts inside a first network to a second network, wherein the NAT facility allows the inside hosts to share an address of the second network;
 - a gateway interface for connecting to a demilitarized zone (DMZ) host inside the first network;
 - a disposer connected to the gateway interface for assigning an address of the second network to the DMZ host in response to a request from the DMZ host, wherein the disposer assigns the second network address of the NAT-enabled device to the DMZ host if such address is public and the disposer assigns a temporary second network address and associated validity lifetime to the DMZ host if the second address of the NAT-enabled device is not public; and
 - a dispatcher connected to the gateway interface and the NAT facility for communicating messages between the second network and the gateway interface or the NAT facility according to a communication criteria of the message, the dispatcher storing the address of the DMZ host and comparing destination address information of a

message received from the second network with the address of the DMZ host, and forwarding the message to the DMZ host when the communication criteria corresponds to the DMZ host and forwarding the message to the NAT facility when the communication criteria does not correspond to the DMZ host, the dispatcher identifying a message being sent to the second network from the DMZ host by checking the communication criteria of such message.

[c10] 10. The NAT-enabled device of claim 9 wherein the communication criteria is derived from a medium access control (MAC) address of the message.

[c11] 11. The NAT-enabled device of claim 10 wherein the disposer allows the DMZ host to acquire a validity lifetime to transmit messages or obtain addresses of hosts in the second network upon a request by the DMZ host.

[c12] 12. A method for communicating information between a first network and a second network, the method comprising:

assigning a second network address to a demilitarized zone (DMZ) host of the first network;

receiving from the second network a message having a destination address equal to the second network address;

forwarding the message to the DMZ host of the first network when a communication criteria of the message matches a first criteria; and
forwarding the message to another host of the first network when the communication criteria of the message does not match criteria.

- [c13] 13. The method of claim 12 wherein the second network address assigned to the DMZ host is the second network address of the first network when such address is public, and the second network address assigned to the DMZ host is a temporary second network address when the second network address of the first network is not public.
- [c14] 14. The method of claim 13 wherein the communication criteria is derived from a medium access control (MAC) address of the message, the first criteria being the MAC address of the DMZ host.
- [c15] 15. The method of claim 14 wherein the temporary second network address has a validity lifetime considerably shorter than that of the second network address of the first network.
- [c16] 16. The method of claim 15 further comprising:
reassigning a second network address to a demilitarized

zone (DMZ) host of the first network upon expiry of the validity lifetime.

- [c17] 17. The method of claim 16 further comprising:
detecting for an active connection between the first and second networks;
activating a connection between the first and second networks when no connection between the first and second networks exists.
- [c18] 18. The method of claim 14 wherein assigning the second network address to the DMZ host is in response to a request from the DMZ host.
- [c19] 19. A network address translation (NAT)-enabled device, gateway device, or network router comprising a NAT facility, a gateway interface, a disposer, and a dispatcher for performing the method of claim 12.